



TITLE:

# On the lower bound of Galois images associated to elliptic curves (Algebraic number theory and related topics)

AUTHOR(S):

新井, 啓介

---

CITATION:

新井, 啓介. On the lower bound of Galois images associated to elliptic curves (Algebraic number theory and related topics). 数理解析研究所講究録 2005, 1451: 275-284

ISSUE DATE:

2005-10

URL:

<http://hdl.handle.net/2433/47746>

RIGHT:

# On the lower bound of Galois images associated to elliptic curves

東京大学大学院数理科学研究科 新井 啓介 (Keisuke Arai)  
Graduate School of Mathematical Sciences, The University  
of Tokyo

## 1 序文

$k$  を標数 0 の体とする.  $G_k$  で  $k$  の絶対ガロア群を表す.  $E$  を  $k$  上の楕円曲線とし,  $N \geq 1$  を自然数,  $p$  を素数とする.  $E$  の  $N$ -等分点のなす群  $E[N]$  への  $G_k$  の作用が定める表現, 及び  $E$  の  $p$  進 Tate 加群  $T_p E$  への  $G_k$  の作用が定める表現をそれぞれ

$$\bar{\rho}_{E,N} : G_k \longrightarrow \text{Aut}(E[N]) \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

$$\rho_{E,p} : G_k \longrightarrow \text{Aut}(T_p E) \cong \text{GL}_2(\mathbb{Z}_p)$$

で表す.

$$1 + p^0 \mathbb{Z}_p^\times := \mathbb{Z}_p^\times, 1 + p^0 \text{M}_2(\mathbb{Z}_p) := \text{GL}_2(\mathbb{Z}_p) \text{ とおく.}$$

**定理 1.1** ([Se1])  $K$  を代数体,  $E$  を虚数乗法をもたない  $K$  上の楕円曲線,  $p$  を素数とする. このとき,

$$\rho_{E,p} : G_K \longrightarrow \text{GL}_2(\mathbb{Z}_p)$$

の像は開である. 即ち,  $K, E, p$  に依存した整数  $n = n(K, E, p) \geq 0$  が存在して,

$$\rho_{E,p}(G_K) \supseteq 1 + p^n \text{M}_2(\mathbb{Z}_p)$$

となる.

私は、上の定理において、べき  $n$  が楕円曲線  $E$  に依存しないようにとれることを示した。即ち、次の定理を証明した。

**定理 1.2**  $K$  を代数体、 $p$  を素数とする。このとき、 $K, p$  に依存した整数  $n = n(K, p) \geq 0$  が存在して、虚数乗法をもたない任意の  $K$  上の楕円曲線  $E$  に対して、

$$\rho_{E,p}(G_K) \supseteq 1 + p^n M_2(\mathbb{Z}_p)$$

が成り立つ。

**注 1.3** 定理 1.2 において、 $n(K, p)$  の  $K, p$  による具体的な評価は、 $K = \mathbb{Q}$  のときでもわかっていない。

## 2 背景

なぜ  $\rho_{E,p}(G_K)$  は  $E$  を動かしても下に有界であろうと思ったか、という研究の動機について例を挙げて説明する。

**定理 2.1** ([Se2])  $K$  を代数体、 $E$  を虚数乗法をもたない  $K$  上の楕円曲線とする。このとき、

$$\prod_{p:\text{素数}} \rho_{E,p} : G_K \longrightarrow \prod_{p:\text{素数}} \mathrm{GL}_2(\mathbb{Z}_p)$$

の像は開である。

**定理 2.2** ([Maz1])  $E$  を  $\mathbb{Q}$  上の楕円曲線とすると、 $E(\mathbb{Q})_{\mathrm{tors}}$  は次のどれかと同型である。

$$\mathbb{Z}/N\mathbb{Z} \quad (1 \leq N \leq 10, N = 12), \quad \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad (1 \leq N \leq 4).$$

**系 2.3**  $E$  を  $\mathbb{Q}$  上の楕円曲線、 $p$  を素数とする。このとき  $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$  が  $\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}$  と共役な部分群に入るとすれば、 $p \leq 7$  が成り立つ。

**定理 2.4** ([Me]) 自然数  $d > 1$  を固定する。  $K$  を  $[K : \mathbb{Q}] = d$  なる代数体、 $E$  を  $K$  上の楕円曲線、 $p$  を素数とする。このとき  $\bar{\rho}_{E,p}(G_K)$  が  $\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}$  と共役な部分群に入るとすれば、 $p < d^{3d^2}$  が成り立つ。

**定理 2.5** ([Pa]) 自然数  $d \geq 1$  を固定する.  $K$  を  $[K : \mathbb{Q}] = d$  なる代数体,  $E$  を  $K$  上の楕円曲線,  $p$  を素数,  $n \geq 1$  を自然数とする. このとき  $\bar{\rho}_{E,p^n}(G_K)$  が  $\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}$  と共役な部分群に入るとすれば,

$$p^n \leq \begin{cases} 65(3^d - 1)(2d)^6 & \text{if } p \geq 5, \\ 65(5^d - 1)(2d)^6 & \text{if } p = 3, \\ 129(3^d - 1)(3d)^6 & \text{if } p = 2 \end{cases}$$

が成り立つ.

**定理 2.6** ([Maz3])  $E$  を  $\mathbb{Q}$  上の楕円曲線,  $p$  を素数とする. このとき  $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$  が  $\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$  と共役な部分群に入るとすれば,  $p \leq 19$  または  $p = 37, 43, 67, 163$  が成り立つ.

**定理 2.7** ([Mo2])  $K$  を 2 次体で, 類数 1 の虚 2 次体ではないとする. このとき自然数  $C = C(K) \geq 1$  が存在して, 次の条件を満たす.  $K$  上の楕円曲線  $E$  と素数  $p$  に対して,  $\bar{\rho}_{E,p}(G_K)$  が  $\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$  と共役な部分群に入るとすれば,  $p < C$  が成り立つ.

**定理 2.8** ([Mo1])  $E$  を  $\mathbb{Q}$  上の楕円曲線,  $p = 11$  又は  $\geq 17$  を素数で,  $\#J_0^-(p)(\mathbb{Q}) < \infty$  が成り立つものとする. このとき  $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$  が  $\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$  と共役な部分群に入り,  $p \neq 37$  とすれば,  $E$  は虚数乗法をもつ.

**定理 2.9** ([Man])  $K$  を代数体,  $p$  を素数とする. このとき, 自然数  $n = n(K, p) \geq 1$  が存在して, 次の条件を満たす.  $K$  上の楕円曲線  $E$  に対し,  $\bar{\rho}_{E,p^n}(G_K)$  が  $\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$  と共役な部分群に入るとすれば,  $E$  は虚数乗法をもつ.

ガロア表現の像が特定の部分群に入るとは, 像が小さくなることであると考えられる. 上記の例たちは, ガロア表現の像がいくらでも小さくなることはない, ということを示唆している.

### 3 主定理

今回の研究の主定理を述べる.

**定理 3.1**  $p$  を素数とする. 整数  $n(p)$  を次のように定義する.

$$n(p) = \begin{cases} 0 & \text{if } p \geq 23, \\ 1 & \text{if } p = 19, 17, 13, 11, \\ 2 & \text{if } p = 7, \\ 3 & \text{if } p = 5, \\ 5 & \text{if } p = 3, \\ 11 & \text{if } p = 2. \end{cases}$$

$K$  を代数体とする. このとき  $p$  に依存した  $K$  の有限部分集合  $\Sigma$  が定まり,  $K$  上の楕円曲線  $E$  で  $j(E) \notin \Sigma$  となるものに対して,

$$\rho_{E,p}(G_K) \supseteq (1 + p^{n(p)} M_2(\mathbb{Z}_p))^{\det=1}$$

が成り立つ. 冒頭で述べたように,  $1 + p^0 M_2(\mathbb{Z}_p) = GL_2(\mathbb{Z}_p)$  とおいている.

さらに,  $G_K$  の  $p$ -進円分指標の像が  $1 + p^r \mathbb{Z}_p$  ( $r \geq 0$ ) を含むとすれば,  $K$  上の楕円曲線  $E$  で  $j(E) \notin \Sigma$  となるものに対して,

$$\rho_{E,p}(G_K) \supseteq 1 + p^{r+n(p)} M_2(\mathbb{Z}_p)$$

が成り立つ. ただし,  $p = 2$  のときは  $r \geq 2$  ととっている. ここで,  $1 + p^0 \mathbb{Z}_p = \mathbb{Z}_p^\times$  とおいている.

**補題 3.2**  $K$  を代数体とする.  $j$  を  $K$  の元で,  $j$ -不変量が  $j$  となるような  $K$  上の楕円曲線は虚数乗法をもたないとする.  $p$  を素数とする. このとき  $j, p$  に依存した整数  $n \geq 0$  が存在して,  $j$ -不変量が  $j$  であるような  $K$  上の任意の楕円曲線  $E$  に対して,

$$\rho_{E,p}(G_K) \supseteq 1 + p^n M_2(\mathbb{Z}_p)$$

が成り立つ.

定理 3.1 と補題 3.2 より定理 1.2 が従う.

注 3.3  $K = \mathbb{Q}$ ,  $p \geq 17$  なら, 有限個の  $j$ -不変量をもつ楕円曲線を除き

$$\rho_{E,p}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}_p)$$

が成り立つ ( $[Fa]$ ,  $[Maz1]$ ,  $[Maz2]$ ).

注 3.4  $K = \mathbb{Q}$  とする.  $p = 13$  なら  $X_0(13) = \mathbb{P}^1$ ,  $\sharp \mathbb{P}^1(\mathbb{Q}) = \infty$  より  $n(13) = 1$  という評価はギリギリである.  $p = 11$  なら  $\sharp X_{\mathrm{non-split}}(11)(\mathbb{Q}) = \infty$  より  $n(11) = 1$  という評価はギリギリである.  $p \leq 7$  のときは  $n(p)$  の評価がギリギリかどうかはわかっていない.

## 4 モジュラー曲線

楕円曲線は, モジュラー曲線の有理点と結び付けて考えることができる. 楕円曲線のガロア表現の像が下に有界であることを, モジュラー曲線の有理点の有限性に帰着して示す. この節では, そのための準備をする.

$N \geq 1$  を自然数とする.  $Y(N)$  を楕円曲線  $E$  とそのレベル  $N$ -構造

$$\alpha: (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\cong} E[N]$$

の組  $(E, \alpha)$  の粗モジュライとする. ( $N \geq 3$  なら  $Y(N)$  は精モジュライである).  $Y(N)$  は  $\mathbb{Q}(\zeta_N)$  上のアファイン, スムーズ代数曲線である.  $G = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$  の部分群  $H$  に対し,  $Y_H$  を商  $Y(N)/H$  と定める.  $X_H$  を  $Y_H$  のスムーズなコンパクト化とする.  $X_H$  は  $\mathbb{Q}(\zeta_N)$  上の固有スムーズ代数曲線である.

補題 4.1  $k$  を標数 0 の体とする.  $\sharp X_H(k) < \infty$  とすると, 有限部分集合  $\Sigma \subseteq k$  で次の条件を満たすものが存在する.  $k$  上の楕円曲線  $E$  に対し  $\bar{\rho}_{E,N}(G_K)$  が  $H$  と共役な部分群に入れば,  $j(E) \in \Sigma$  が成り立つ.

次の定理は, Mordell 予想と呼ばれていて, 種数が 2 以上の固有スムーズ代数曲線の有理点の有限性を示すものであり, 定理 3.1 の証明の鍵となっている.

定理 4.2 ( $[Fa]$ )  $K$  を代数体,  $X$  を  $K$  上の固有スムーズ代数曲線とする.  $g(X) \geq 2$  と仮定する. このとき  $\sharp X(K) < \infty$  が成り立つ.

$H \ni -1$  のとき,  $X_H$  の種数  $g(X_H)$  は Riemann-Hurwitz の公式を用いて次のように計算される.

$$g(X_H) = 1 + \frac{1}{12} \#G/H - \frac{1}{4} \# \text{Fix}_\sigma - \frac{1}{3} \# \text{Fix}_\tau - \frac{1}{2} \# \langle u \rangle \backslash G/H.$$

但し

$$\sigma := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\tau := \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

$$u := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\text{Fix}_\alpha := \{gH \in G/H \mid \alpha gH = gH\}$$

とおいている.

## 5 証明の概略

簡単のため, 以下  $p \geq 5$  とする.

**補題 5.1**  $H \subseteq \text{SL}_2(\mathbb{Z}_p)$  を閉部分群,  $n \geq 0$  を整数とする. このとき,  $H \supseteq (1 + p^n \text{M}_2(\mathbb{Z}_p))^{\det=1}$  であるための必要十分条件は,  $H \bmod p^{n+1} \supseteq (1 + p^n \text{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}))^{\det=1}$  が成り立つことである. ここで,  $1 + p^0 \text{M}_2(\mathbb{Z}/p\mathbb{Z}) := \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$  とおいている.

$K$  を  $K(\zeta_{p^{n(p)+1}})$  で置きかえて,  $K$  上の任意の楕円曲線  $E$  に対して

$$\det \bar{\rho}_{E, p^{n(p)+1}}(G_K) = \{1\}$$

が成り立つようにする. 定理 3.1 を示すには, 部分群  $H \subseteq G = \text{SL}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z})$  で条件  $H \ni -1$ ,

$$H \not\supseteq (1 + p^{n(p)} \text{M}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z}))^{\det=1} \quad (5.1)$$

を満たすものについて  $g(X_H) \geq 2$  を示せばよい. 種数  $g(X_H)$  は次のように書き換えられる.

$$g(X_H) = 1 + \frac{1}{12} [G : H] \delta_H,$$

但し

$$\delta_H := 1 - 3 \frac{\#H \cap \text{Conj}(\sigma)}{\#\text{Conj}(\sigma)} - 4 \frac{\#H \cap \text{Conj}(\tau)}{\#\text{Conj}(\tau)} - 6 \left( \frac{1}{p^{n(p)+1}} + \sum_{r=0}^{n(p)} \frac{p-1}{p^{r+1}} \cdot \frac{\#H \cap \text{Conj}(u^{p^r})}{\#\text{Conj}(u^{p^r})} \right),$$

$$\text{Conj}(\alpha) := \{g \in G \mid g \text{ は } \alpha \text{ と共役}\}$$

とおいている. 種数  $g(X_H)$  は整数であるから,  $g(X_H) \geq 2$  という条件は  $\delta_H > 0$  という条件と同値である.  $\#H \cap \text{Conj}(\sigma)$ ,  $\#H \cap \text{Conj}(\tau)$ ,  $\#H \cap \text{Conj}(u^{p^r})$  を条件 (5.1)

$$H \not\subseteq (1 + p^{n(p)} M_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z}))^{\det=1}$$

を用いて上から抑える. 自然数  $1 \leq t < s \leq n(p) + 1$  に対し,  $\text{mod } p^t$  写像

$$H \bmod p^s \longrightarrow H \bmod p^t$$

による  $\sigma, \tau, u^{p^r}$  の共役元の逆像の大きさを抑えるという方針をとる.

自然数  $1 \leq m < n$  に対し,

$$f_{n,m} : \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \text{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$$

を  $\text{mod } p^m$  写像とする.  $\alpha = \sigma, \tau$  に対し,

$$V_\alpha^{n,m} := \alpha^{-1}(f_{n,m}^{-1}(\alpha) \cap \text{Conj}(\alpha)) \subseteq \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

とおく.

**補題 5.2**  $n \leq 2m$  と仮定する. このとき,

$$V_\sigma^{n,m} = \left\{ 1 + p^m \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \right\},$$

$$V_\tau^{n,m} = \left\{ 1 + p^m \begin{pmatrix} a & b \\ b-a & -a \end{pmatrix} \right\},$$

となり, これらは階数 2 の自由  $\mathbb{Z}/p^{n-m}\mathbb{Z}$  加群の構造をもつ.



$\sigma, \tau$  と共役な元  $\alpha \in \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$  に対しても同様に  $V_\alpha^{n,m}$  が定義され、階数 2 の自由  $\mathbb{Z}/p^{n-m}\mathbb{Z}$  加群の構造をもつ。

$r \geq 0$  を整数とする。

$$V_{u^{p^r}}^{r+n, r+m} := u^{-p^r} (f_{r+n, r+m}^{-1}(u^{p^r}) \cap \mathrm{Conj}(u^{p^r})) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$$

とおく。

**補題 5.3**  $n \leq 2m$  と仮定する。このとき、

$$V_{u^{p^r}}^{r+n, r+m} = \left\{ 1 + p^{r+m} \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} \right\}$$

となり、これは階数 2 の自由  $\mathbb{Z}/p^{n-m}\mathbb{Z}$  加群の構造をもつ。

$u^{p^r}$  と共役な元  $\alpha \in \mathrm{SL}_2(\mathbb{Z}/p^{r+m}\mathbb{Z})$  に対しても同様に  $V_\alpha^{r+n, r+m}$  が定義され、階数 2 の自由  $\mathbb{Z}/p^{n-m}\mathbb{Z}$  加群の構造をもつ。

自然数  $1 \leq s \leq n(p) + 1$  に対し、

$$H_s := H \cap (1 + p^s \mathrm{M}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z})) = \mathrm{Ker}(\mathrm{mod } p^s : H \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z}))$$

とおく。  $H/H_s$  と  $H \bmod p^s$  を同一視する。自然数  $1 \leq t < s \leq n(p) + 1$  と  $\alpha = \sigma, \tau, u^{p^r}$  に対し、

$$f_{s,t}^{H,\alpha} : (H/H_s) \cap \mathrm{Conj}(\alpha) \longrightarrow (H/H_t) \cap \mathrm{Conj}(\alpha)$$

を  $\mathrm{mod } p^t$  写像とする。ここで、 $\alpha = u^{p^r}$  のときは、 $t > r$  と仮定している。条件 (5.1) により

$$\#H_t/H_s \leq p^{2(s-t)}$$

が成り立つ。

**補題 5.4** 自然数  $1 \leq t < s \leq n(p) + 1$  をとり、 $s \leq 2t$  と仮定する。 $\alpha$  を  $\sigma, \tau, u^{p^r}$  のいずれかとし、 $(H/H_t) \cap \mathrm{Conj}(\alpha)$  の元  $\alpha'$  をとる。もし  $H_t/H_s = V_{\alpha'}^{s,t}$  なら、 $\#(f_{s,t}^{H,\alpha})^{-1}(\alpha') = p^{2(s-t)}$  が成り立つ。もし  $H_t/H_s \neq V_{\alpha'}^{s,t}$  なら、 $\#(f_{s,t}^{H,\alpha})^{-1}(\alpha') \leq p^{2(s-t)-1}$  が成り立つ。

**補題 5.5** 自然数  $1 \leq t < s$  をとり、 $s \leq 2t$  と仮定する。

1.  $\sigma', \sigma'' \in \mathrm{Conj}(\sigma) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^t\mathbb{Z})$  をとる。このとき、 $V_{\sigma'}^{s,t} = V_{\sigma''}^{s,t}$  となるための必要十分条件は、 $\sigma'' \equiv \sigma'^{\pm 1} \bmod p^{s-t}$  が成り立つことである。

2.  $\tau', \tau'' \in \text{Conj}(\tau) \subseteq \text{SL}_2(\mathbb{Z}/p^t\mathbb{Z})$  をとる. このとき,  $V_{\tau'}^{s,t} = V_{\tau''}^{s,t}$  となるための必要十分条件は,  $\tau'' \equiv \tau'^{\pm 1} \pmod{p^{s-t}}$  が成り立つことである.

3.  $v, v' \in \text{Conj}(u^{p^r}) \subseteq \text{SL}_2(\mathbb{Z}/p^{r+t}\mathbb{Z})$  をとる. このとき,  $V_v^{s,t} = V_{v'}^{s,t}$  となるための必要十分条件は, ある  $p$  と素な自然数  $i$  に対して  $v' \equiv v^{i^2} \pmod{p^{r+s-t}}$  が成り立つことである.

補題 5.4, 5.5 を用いると,  $f_{s,t}^{H,\alpha}$  による  $(H/H_t) \cap \text{Conj}(\alpha)$  の逆像  $(H/H_s) \cap \text{Conj}(\alpha)$  の元の数を抑えることができる.

また  $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$  の極大部分群の分類 ([Se2]) を利用して,  $H/H_1$  の中の  $\sigma, \tau, u$  の共役元の数を抑える.

以上のようにして  $\delta_H > 0$  が示され, 定理 3.1 が証明される.

## 参考文献

- [Fa] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Translated from the German original [Invent. Math. 73 (1983), no. 3, 349-366; ibid. 75 (1984), no. 2, 381] by Edward Shipz. Arithmetic geometry (Storrs, Conn., 1984), 9-27, Springer, New York (1986).
- [Man] J. Manin, *The  $p$ -torsion of elliptic curves is uniformly bounded*, Translated from the Russian original [Izv. Akad. Nauk SSSR Ser. Mat. 33 1969 459-465]. Mathematics of the USSR-Izvestija, Vol. 3 (1969), No. 3-4, 433-438.
- [Maz1] B. Mazur, *Modular curves and the Eisenstein ideal*, I.H.E.S. Publ. Math. No. 47 (1977), 33-186.
- [Maz2] B. Mazur, *Rational points on modular curves*, Modular functions of one variable V, Lecture Notes in Math., Vol. 601, Springer, Berlin (1977), 107-148.
- [Maz3] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129-162.
- [Me] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), no. 1-3, 437-449.

- [Mo1] F. Momose, *Rational points on the modular curves  $X_{\text{split}}(p)$* , Compositio Math. 52 (1984), no. 1, 115–137.
- [Mo2] F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. 97 (1995), no. 3, 329–348.
- [Pa] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116.
- [Se1] J.-P. Serre, *Abelian  $l$ -adic representations and elliptic curves*, Lecture at McGill University, New York-Amsterdam, W. A. Benjamin Inc. (1968).
- [Se2] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), no. 4, 259–331.